Exhibit 7

Declaration of James Van Dyke

In re: Equifax Inc. Customer Data Security Breach Litigation,
No. 17-md-2800-TWT (N.D. Ga.)

Plaintiffs' Motion to Direct Notice of Proposed Settlement

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF GEORGIA

ATLANTA DIVISION

IN RE:	)	
	)	**Case No.: 1:17-md-02800-TWT**
Equifax, Inc., Customer Data	)	
Security Breach Litigation	)	**Consumer Actions**
	)	
	)	

Declaration of James Van Dyke

I. Introduction and Relevant Qualifications

I, James Van Dyke, pursuant to 28 U.S.C. § 1746 hereby declare as follows:

1. I am the Founder and CEO of Futurion.digital, Inc., a research-based consulting firm specializing in areas including consumer identity fraud and security, as well as financial and payments technology. I am also the founder, CEO, and inventor of Breach Clarity, launched in March of 2019 to compute risks and recommend action steps for all publicly-reported US data breaches (currently covering January 2017 to the present, plus some earlier prominent breaches).[1] I currently serve on the Board of Directors of The Identity theft Resource Center, a 501(c)3 non-profit focused on mitigating consumer risks created by data breaches. From 2013 to 2016, I also served on the Consumer Advisory Board of the Consumer Financial Protection Bureau—an agency of the United States responsible for consumer protection in the financial sector. Prior to establishing Futurion, I founded and served as CEO of Javelin Strategy & Research, a leading provider of quantitative and qualitative research on subjects including consumer security, fraud, digital banking, payments, and financial transaction innovation. Before that, I started the financial services research unit of Jupiter Research, a New York company providing similar offerings to Javelin's.

[1] Any outputs from the publicly-available free, algorithm-driven, and extremely high-level version of Breach Clarity are not intended to in any way be a substitute for my in-depth and personalized opinion that was created for this or any other expert witness report through my traditional research methods.

2. My pertinent qualifications include substantial research and leadership in the fields of fraud and security, particularly harms including identity theft and fraud that result from data compromise. This expertise builds on over a decade of conducting and publishing primary research of consumers, banks, merchants, and vendor-solutions directly concerned with the subject of consumer identity theft and the enabling act of personal data compromise. This research was primarily purchased by organizations that sought to mitigate or minimize the damage from identity crimes, such as financial institutions, merchants, government agencies, and specialty vendors.

3. Directly, or through my staff members, I have provided strategic and research-driven advice to most of the nation's largest consumer financial institutions, retail financial tech-sector vendors, as well as a select number of identity-protection services vendors who generally are focused on creating services that empower or protect consumers' financial health.

4. I have a Bachelor of Science degree from San Jose State University and a Master of Business Administration from Golden Gate University—both of which I earned with honors.

5. My former company, Javelin Strategy & Research, is the leading provider of research on the subject of consumers' experience in harms stemming from compromise of personal identity data, including identity theft or fraud and

other related topics, which includes a focus on financial services and payment transaction systems (because this is one area where identity criminals frequently seek to profit from the results of data compromise).[2] Javelin continues to be known for its industry-leading, rigorous, and annually-recurring research studies of consumer financial services behaviors, attitudes, industry practices, and technology trends, related to such topics as mobile banking, personal financial management, payments, security, cybercrime, and identity fraud or theft. In particular, Javelin uniquely provides annual primary research-based studies of the consumer, business, and financial services impact of identity theft and fraud, including its link to data compromise.

[2] In 2012, I sold 100% of my interest in the company to Greenwich Associates, a privately-held research company focused on commercial financial institution operations. I concluded my post-sale relationship with Javelin on December 31, 2015. Javelin's studies represent the largest body of available identity-theft research, with at least four major methodologies: 1) surveying over 5,000 consumers each year to assess the latest patterns of identity crimes, along with the relationship to the enabling component of data compromise (such as data breaches); 2) merchants' experiences with consumer identity theft; 3) bank efforts to empower consumers to protect themselves against identity fraud and related security incidents; and 4) a comparison of identity-protection service providers. Because Javelin produces some of the most rigorous and widely-cited studies on identity theft, I cite them frequently. First published in 2005 to build on methodologies created by the Federal Trade Commission, Javelin's annual identity-theft survey report asks consumers a wide variety of questions related to their experiences with identity fraud or other misuse, notifications of data breaches, and practices related to security, payments, and other areas of financial services. Over the years, over 50,000 consumers have been cumulatively surveyed in the annual Javelin identity theft reports. Javelin's work was under my supervision through December 31, 2015. In Appendix A of this study, I have provided a methodology statement for Javelin's most significant report, the Identity Theft Survey Report, which is cited extensively in this report because it is the nation's only annually-deployed and nationally-representative consumer identity fraud survey.

6. Original research from Javelin is used or has been cited by the U.S. Congress,[3] Consumer Financial Protection Bureau,[4] United States Department of Justice,[5] Board of Governors of the Federal Reserve System,[6] regional Federal Reserve banks,[7] the Federal Deposit Insurance Corporation,[8] the U.S. Department of the Treasury, Federal Trade Commission,[9] and all or nearly all of the largest banks, payments firms, and associated financial technology vendors operating in the United States.

7. I have been interviewed for hundreds of news media articles or featured stories including Bloomberg, Financial Times, Fox News live television, National Public Radio (NPR), the front page of The New York Times, The Washington Post, and Wired. The widest coverage of my research-based opinions has been on the subject of identity theft or fraud, and in particular in response to research released under my supervision that surveys consumer fraud victims or benchmarks bank and merchants' efforts to fight identity theft.

[3] https://fas.org/sgp/crs/misc/R40599.pdf
[4] https://files.consumerfinance.gov/f/201511_cfpb_mobile-financial-services.pdf
[5] https://www.justice.gov/sites/default/files/usao/legacy/2008/04/16/usab5602.pdf
[6] https://www.federalreserve.gov/pubs/bulletin/2012/articles/MobileFinancialServices/mobile-financial-services.htm#f24
[7] https://www.frbatlanta.org/-/media/documents/rprf/rprf_pubs/130408surveypaper.pdf
[8] https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin12/siwinter12-article1.pdf
[9] https://www.ftc.gov/system/files/documents/public_comments/2017/10/00008-141502.pdf

8. Within at least the last four years, I have testified as an expert at trial or by deposition in numerous data breach cases.

II. Scope of Assignment & Compensation

9. I have been asked by Consumer Plaintiffs' counsel to evaluate the Identity Theft Protection Solution (IDPS) being offered as part of the proposed settlement of this class action and opine on its suitability for the harms that Equifax data breach victims are likely to face as a result of the breach.

10. Consumer Plaintiffs' counsel are compensating me at my standard hourly rate. No aspect of my compensation depends upon my reaching any particular conclusions or on the outcome of this case.

11. I have personal knowledge of the facts set forth below, or I am informed of certain facts as described below based on my review of documents or discussions with counsel for Consumer Plaintiffs. If called to testify, I could and would do so competently.

III. Individuals Whose Personal Data Is Compromised Experience Increased Risks Resulting from that Compromise

12. Individuals whose personal data is comprised are subject to increased risk because of that compromise. Without a data breach or other data exposure, there can generally be no fraud, "identity theft", or other personal information misuse. This is true because unauthorized access to PII is what makes identity fraud (sometimes called "identity theft") possible. Furthermore, *increased* access to private data—either in the form of repeated breaches or increased breadth of exposures—increases the risk of injury to levels above what they otherwise would have been.[10]

13. Consumer victims of data breaches are much more likely to become victims of identity fraud. For example, individuals who reported that they were victims of one or more data breaches were also more likely to report being a victim of identity fraud.[11]

14. The average victim of identity theft or fraud pays a significant personal toll. Identity theft or fraud often directly causes unreimbursed losses such as legal fees, bounced checks, late charges, service reinstatement fees, credit

[10] *Rising Number of Data Breaches Increases Threat of Identity Fraud* http://consumerfed.org/press_release/rising-number-data-breaches-increases-threat-identity-fraud/, Sept 06, 2016.
[11] 2014 LexisNexis True Cost of Fraud Study, https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf, accessed May 14, 2019.

freezes, and other related expenses (e.g., copying, postage, notary fees). Some victims pay fraudulent debts to avoid further problems. Importantly, multiple government, private sector, and non-profit organization research studies have reported on the emotional toll from which victims of identity theft and fraud suffer.

15. Fraud figures for any given year add up to a substantial amount of crime, representing losses to commercial organizations, individuals, and others. For instance, in 2016 the face-value total of all identity fraud incidents encountered by 15.4 million victims of identity fraud in 2016 was $16 billion.[12]

IV. The Immutable Data Taken in the Equifax Breach Place Victims At Risk In Perpetuity

16. According to Equifax's SEC filings, nearly all of the Equifax data breach victims in the U.S. had their name, date of birth, and Social Security number taken by the hackers.[13] Because these credentials are of a persistent nature—meaning they cannot be changed—these individuals will remain at a heightened risk of identity theft for the rest of their lives. And every additional data point taken increases the breach victim's exposure. The chart below lists the numbers of U.S. consumers who had each type of data taken:[14]

[12] https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new
[13] https://www.sec.gov/Archives/edgar/data/33185/000119312518154706/d583804d8k.htm
[14] *Id.*

Type of Data Taken	**Approximate Number of U.S. Consumers Affected**
Name	146.6 million
Date of Birth	146.6 million
Social Security Number	145.5 million
Address	99 million
Gender	27.3 million
Phone Number	20.3 million
Drivers License Number	17.6 million
Email Address	1.8 million
Payment Card Information	209,000
Tax ID	97,500
Drivers License State	27,000

17. These types of data are commonly used by criminals in a variety of ways. First, the data can be combined with information from other sources to create detailed identity profiles, of 'fullz,' which command a price premium in criminal marketplaces. Because these illicit marketplaces have become pervasive, particularly on the global dark web (also called the 'dark net'), criminals can either use the data to commit fraud immediately or offer it for sale at various points of time in the future (which in turn enables it to be used for other frauds at some future point in time).

18. In fact, the specific credentials taken on over 99% of Equifax breach victims – names, dates of birth, and Social Security numbers – are often termed

"The Holy Trinity,"[15] because they so effectively (or even foundationally) work together as the basis for criminal identity misuse.

V. Types of Fraud Equifax Breach Victims Are Most Likely to Suffer

19. The types of fraud that Equifax breach victims are most likely to suffer include financial account fraud, tax refund fraud, account takeover fraud, criminal identity theft, and phone / utility fraud.

20. New account fraud (NAF) generally refers to the act of fraudulently opening accounts, usually financial accounts, with the goal of conducting expensive transactions that are ultimately charged to the victim. NAF is strongly correlated to Social Security number (SSN) breaches, particularly where the SSNs are paired with corroborating information like name, date of birth, and address.

21. One of the pernicious aspects of NAF is that it often takes victims an exceedingly long time to even realize that a new account has been opened in their name. Victims often discover the accounts when they are contacted by debt collection agencies (and often after the victims have had their credit scores lowered). In 2016, NAF victims spent on average over $150 and 15 hours

[15] Dr. Daniel Dimov, *Identity Theft:, The Means, Methods and Recourse*, Infosec Institute, https://resources.infosecinstitute.com/identity-theft-means-methods-recourse/#gref, January 14, 2013.

responding to the fraud.[16] SSN breach victims face more than 5 times more new account fraud than all average US adults.[17]

22. Tax refund fraud

a. Due to the PII exposed, the Equifax data breach victims face increased risk of tax refund fraud, in which criminals impersonate the victim and a file false tax return to obtain a tax refund in their name. The GAO reports that there was $3.1B paid out in fraudulent IRS tax returns in 2014.[18].

b. Tax fraud occurs when criminals file fraudulent tax returns in another individual's name, in order to obtain a refund owing to that individual. This occurs after an identity criminal obtains necessary PII (which includes name, SSN, and DOB) and uses it to create fake tax returns that appear convincing enough to result in distribution of the payment. Criminals cash the refund check before the authentic taxpayer has time to submit their own genuine version. Tax fraud also causes significant delays in receipt of funds owed to "true name"[19] consumers.

c. Consumers can experience debilitating financial impact from tax refund fraud, which can require substantial investment of time to resolve, and

---

[16] *2017 Identity Fraud: Securing the Connected Life*, Javelin Strategy & Research.
[17] *2016 Data Breach Fraud Impact Report,* Javelin Strategy & Research, page 15.
[18] *IDENTITY THEFT AND TAX FRAUD,* GAO, http://www.gao.gov/assets/680/677405.pdf, May 2016.
[19] 'True name' is a label used by fraud mitigation professionals to refer to the legitimate identity holder, in contrast to one or more 'fraudsters' who are impersonating them.

frequently delays their receiving refunds correctly owed to them. As the IRS has stated: "[i]nnocent taxpayers are victimized because their refunds are delayed."[20] A report from the Treasury Department confirms that "the IRS informs taxpayers who inquire about the status of their identity theft case that cases are resolved within 180 days," yet the report goes on to cite its own "statistically-valid sample" in finding that "Resolution averaged 312 days with tax accounts assigned to an average of 10 assistors during processing. In addition, 25 percent (of) tax accounts were not correctly resolved, resulting in (further) delayed and incorrect refunds."[21]

23. Account takeover fraud

a. Account takeover (ATO) of financial or other accounts is another risk now faced by the victims of the Equifax data breach. ATO occurs when the fraudster gains compromised credentials to access a victim's existing financial and other accounts to create fraudulent transactions, and by definition generally involves changing the victim's contact information. Equifax's data breach compromised several mostly persistent identifiers including names, addresses, and most importantly SSNs, which are frequently used by customer service representatives or automated authentication systems to verify identities.

[20] https://www.irs.gov/uac/newsroom/tips-for-taxpayers-victims-about-identity-theft-and-tax-returns-2014 January 2014.
[21] *Victims Of Identity Theft Continue To Experience Delays And Errors In Receiving Refunds*, U.S. Treasury, https://www.treasury.gov/tigta/auditreports/2015reports/201540024fr.pdf , March 20, 2015.

b. Criminal use of compromised PII to change account settings and take over an existing account has grown significantly in recent years. A total of $5.1 billion in ATO losses were reported in 2017, a 120 percent increase from the prior year.

c. ATO is one of the most damaging of fraud types for victims, who pay an average of $290 in out-of-pocket costs and spend an average of 16 hours resolving the crime. In 2017, ATO victims devoted more than 62.2 million hours to resolving issues from ATO fraud.[22] PII, particularly the types of data taken in the Equifax breach, is used to perpetrate ATO because financial providers use SSNs and such information to authenticate the identity-holder.

24. Existing account fraud

a. Existing account non-card fraud (ENCF) occurs when individuals suffer fraud within a non-card account that they legitimately opened, generally a financial account such as a depository bank account, investment account, internet account (e.g., Amazon or PayPal), utility account, or medical account. In 2017, ENCF victims suffered average out-of-pocket losses of $160.[23] The key to enable this type of fraudulent conduct, as with other types of fraud, is access to the consumer's SSN. The risk of both new and existing account fraud

[22] https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin# .
[23] *2017 Identity Fraud: Securing the Connected Life,* Javelin Strategy & Research

(including card and non-card accounts) is increased for the victims of Equifax's data breach because the breach released the "holy trinity" of data criminals generally require to carry out their fraud.

25. Risks to minors

a. When minors have their private data exposed in a breach–as happened to millions of children in Equifax's data breach, the –risk of what is sometimes called 'child identity theft' increases in ways that bear resemblance to that of adults. The most current nationally-representative study on child identity theft—commissioned by Identity Guard and conducted by Javelin Strategy & Research—found:

i. In 2017, there were over one million child identity fraud victims;

ii. The fraud losses incurred totaled $2.4 billion;

iii. Out of pocket losses to victims and their families were $540 million; and

iv. The average child identity theft losses were particularly severe, likely because children are not yet active managers of their own financial affairs and thus not generally able to mitigate the risk of such crimes, like an adult would. The average child identity theft victim suffered over $500 in out-of-pocket losses, requiring over 20 hours of resolution time

(usually incurred by a parent). The total average fraud amount (covering all fraud types) for child identity theft victims was over $2,000.[24] For comparison purposes, the 2017 Javelin report on adult identity theft reports a mean out-of-pocket cost of more than $40, more than 5 hours spent on resolution, and a total average fraud amount was over $1,000.[25] This contrast illustrates that child identity theft risks that are made more likely as a result of a data breach should not be ignored even though the overall incident rate of identity crimes against minors is generally lower than that for adults.

b. Prior research studies conducted by Javelin have found that Social Security numbers are highly correlated with child identity theft, and also that crimes are more difficult to detect and resolve than adult ID fraud, at 334 days to detect, and 17% of children were victimized for a year or longer.[26]

26. Other relevant categories or methods of identity misuse and harms include"

[24] *2018 Child Identity Fraud Study*, Javelin Strategy & Research, page 7.
[25] *2017 Identity Fraud: Securing the Connected Life,* Javelin Strategy & Research, page 16.
[26] *ITAC Child ID Fraud Survey Report*, https://www.prweb.com/releases/2012/12/prweb10197105.htm , announced December 4, 2012.

a. Employment or wage-related fraud (which is part of the 82,051 self-reported 'employment and tax-related fraud' crimes in 2017 tracked by the FTC[27]);

b. Phone or utilities fraud (55,045 reported to the FTC);[28]

c. Government documents or benefits (25,849 self-reported victims in the same study);[29]

d. Evading the law (also called 'criminal identity theft'). As accessed from the FTC's web site, "Criminal identity theft occurs when certain credentials are presented to law enforcement (and) the results could be criminal record or arrest warrants. The consumer may never know until they are stopped for a driving violation and realize there is an arrest warrant in their name."[30]

e. Other account misuse–in all manner of accounts such as Amazon, Netflix, discussion boards, social media accounts, and nearly any other type of service not discussed above–can lead to a broad range of harms, including interruption of service, embarrassment, and reputation damage, hours of resolution time, and out-of-pocket financial losses. This final 'catch-all' category of identity

---

[27] *Consumer Sentinel Network*, March 2018, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf Federal Trade Commission.
[28] Ibid.
[29] Ibid
[30] Lanny Britnell, Identity Theft America, *The Changing Face of Identity Theft,* https://www.ftc.gov/sites/default/files/documents/public_comments/credit-report-freezes-534030-00033/534030-00033.pdf , accessed May 15, 2019

misuse also results from breached identity credentials being used in 'social engineering' or knowledge-based authentication attacks. In these attacks, criminals convince customer service personnel or an organization's self-service systems that a criminal is the breached identity holder.

VI. IDPS Provided in The Proposed Equifax Data Breach Settlement

27. At the request of Consumer Plaintiffs' counsel, I have reviewed the contract governing the IDPS services to be provided under the proposed settlement. Below, I summarize the key features and explain the potential and relative benefits of each.

28. IDPS Vendor. The Settlement Agreement proposes using Experian. Experian is a large player in the IDPS market. Accordingly, I expect that it will have the resources to service a class of this magnitude without being swamped.

29. Credit Monitoring Services. Experian will provide three-bureau credit monitoring and alerting and provide consumer reports to class members on a monthly basis. Though many IDPS monitor only one bureau, the most effective solutions monitor each of the three major credit bureaus. As a convenience, the proposed IDPS would permit the class members to obtain their full Experian credit reports for free on a monthly basis.

30. I expect that the proposed IDPS will be a substantial beneficial to class members in protecting their privacy, particularly in the early detection of new

account fraud and account takeover fraud. By alerting on credit inquiries and new accounts being opened, the class member will be able to close down new accounts quickly. The IDPS also would alert on changes to the class members' address, which is useful in stopping account takeover fraud.

a. Early Warning System Alerts. This feature provides almost instantaneous notifications when a class member's PII is used to open or apply for a new account. This is a very valuable feature for class members. These types of early warning systems help prevent or detect New Account Fraud, and are particularly useful in detecting the opening of high-risk financial accounts. This feature, which is generally reserved for 'high end' IDPS packages, is very beneficial for class members.

b. Unusual Credit Activity Alerts. This set of services would warn class members when unusual credit activity is detected. For example, if the class member's credit limits, balances, or utilization increase or decrease by a certain threshold, the class member will receive an alert about the change. Or when an inactive or dormant credit account suddenly reports a balance, the class member will be notified and able to respond. These are important features that are easy to miss by a person or service casually reviewing a credit report, and are beneficial to the class members.

31. Non Credit Protections. The proposed IDPS also would monitor for types of fraud that traditional credit monitoring would miss. This monitoring, though often omitted from less sophisticated IDPS products, is at least as important as true credit monitoring to preventing identity fraud. Below, I list the key non-credit protections under the proposed IDPS.

a. Account Takeover Notifications. Chief among the non-credit protections offered in the proposed IDPS is financial account takeover notification. This type of service monitors the class member's bank accounts for changes to the contact and other profile information and for attempts to open new, linked accounts. This is one of the most important protections for Equifax data breach victims to obtain and would confer a substantial benefit.

b. Change of Address (COA) Notifications. This notifies the individual if his or her postal address is surreptitiously changed, which is one technique used in carrying out various other types of identity fraud.

c. Court Records Notifications. This type of monitoring searches for the individual's credentials in a variety of criminal and court records. This is one of the few ways of detecting criminal identity fraud before the individual is wrongly arrested or fined.

d. Social Security Number Tracing. This type of investigation searches through public records to determine if a class member's SSN is being

used, particularly in connection with other identities. This is very useful in detecting the use of a class member's information in a "synthetic identity," a fake identity generally made of composite PII from several people. Without this type of service synthetic identity theft is usually very difficult for an individual to detect.

e. Dark Web Monitoring. As the name suggests, this is a service in which the IDPS vendor or its affiliates search for the individual's information on the dark web and alerts if that information is found. Dark web searches cannot currently provide comprehensive monitoring because illicit identity marketplaces are designed to hamper comprehensive surveillance. Nonetheless, this is a beneficial technology that will improve throughout the long duration of the settlement.

f. Pay-day loan notifications. Pay-day loan and other unsecured credit services often do not check the borrower's credit files and are invisible to traditional credit monitoring services. This IDPS, however is able to monitor pay-day loan applications and report when the class member's SSN is used.

32. Child Monitoring. The IDPS services also provides special monitoring for minors. Because minors often lack credit files, they are more difficult to protect. The proposed IDPS addresses this issue by providing minors dark web monitoring, SSN trace and credit header monitoring, along with identity theft restoration and ID theft insurance. In addition, when the minor reaches age 18, he

or she can enroll in the adult IDPS product. This is an important set of protections for a vulnerable population.

33. Miscellaneous Details. Finally, I appreciate that the proposed IDPS allows class members to obtain the benefits on their own terms. Many IDPS are available only to individuals who can use the vendor's website or receive email notifications. Because people who have suffered from identity fraud are understandably reluctant to provide PII over the internet, even if it will help protect them, I am pleased to see that this feature was included.

34. Identity Theft Insurance. Identity theft insurance provides additional potential value for class members, for instance in extreme cases where fraud victims encountered extreme unreimbursable costs associated with restoring their identity.

35. Identity Restoration Services. Identity restoration services provide for dedicated representatives who can advise identity theft victims on the steps needed to remedy the fraud and in some cases even act directly on the victim's behalf. This concierge service provides some measure of additional value because it is available to the entire class, not just those people who sign up for the IDPS product.

36. As the above discussion demonstrates, the IDPS in the proposed settlement includes a full suite of services that are tailored to address the type of

information taken in the Equifax data breach, and the ramifications of the misuse of that information. In the current retail market, I would expect this product to cost at least $25 per-person per-month, with the amount increasing over the duration of the settlement. In short, it is my opinion that the IDPS and ID restoration services made available to class members under the settlement provide valuable relief and are tailored to redress the types of injuries that class members may experience as a result of their data having been exposed in the breach.

I declare under penalty of perjury, under the laws of the United States of America, that the above statements are true and correct.

Executed on this the 21st day of July, 2019, in Aruba.

JAMES VAN DYKE